Godfrey Nolan

Bulletproof Android™

Practical Advice for Building Secure Apps

Bulletproof Android™

Bulletproof Android: Practical Advice for Building Secure Apps

Table of Contents

Contents

Preface

Acknowledgments

About the Author

1 Android Security Issues

Why Android?

Decompiling an APK

Art for Arts Sake

Guidelines

PCI Mobile Payment Acceptance Security Guidelines

Google Security

HIPAA Secure

OWASP Top 10 Mobile Risks (2014)

Forrester Researchs Top 10 Nontechnical Security Issues in Mobile App Development

Securing the Device

SEAndroid

Federal Information Processing Standard (FIPS)

Conclusion

2 Protecting Your Code

Looking into the classes.dex File

Pearson

Table of Contents

- Obfuscation Best Practices
  - No Obfuscation
  - ProGuard
  - DexGuard
  - Security Through Obscurity
  - Testing
- Smali
  - Helloworld
  - Remove App Store Check
- Hiding Business Rules in the NDK
- Conclusion

3 Authentication

- Secure Logins
- Understanding Best Practices for User Authentication and Account Validation
  - Take 1
  - Take 2
  - Take 3
  - Take 4
- Application Licensing with LVL
- OAuth
  - OAuth with Facebook
  - Web and Mobile Session Management
  - Vulnerability
- User Behavior
  - Two (or More) Factor Authentication
- Conclusion

Table of Contents

4 Network Communication
- HTTP(S) Connection
- Symmetric Keys
- Asymmetric Keys
- Ineffective SSL
  - Man-in-the-Middle Demo
  - Root Your Phone
  - Charles Proxy Test
- Conclusion

5 Android Databases
- Android Database Security Issues
- SQLite
  - Backing Up the Database Using adb
  - Disabling Backup
- SQLCipher
  - Finding the Key
- Hiding the Key
  - Ask Each Time
  - Shared Preferences
  - In the Code
  - In the NDK
  - Web Services
- SQL Injection
- Conclusion

6 Web Server Attacks
- Web Services
  - OWASP Web Services Cheat Sheet

Table of Contents

Replay Attacks

Cross Platform

WebView Attacks

SQL Injection

XSS

Cloud

OWASP Web Top 10 Risks

OWASP Cloud Top 10 Risks

HIPAA Web Server Compliance

Conclusion

7 Third-Party Library Integration

Transferring the Risk

Permissions

Installing Third-Party Apps

Installing Crittercism

Installing Crashlytics

Trust but Verify

Decompiling SDKs

Man in the Middle

Conclusion

8 Device Security

Wiping Your Device

Fragmentation

adb Backup

Logs

Device Encryption

SEAndroid

Table of Contents

FIPS 140-2

Mobile Device Management

Conclusion

9 The Future

More Sophisticated Attacks

Internet of Things

Android Wearables

Ford Sync AppID

Audits and Compliance

Tools

Drozer

OWASP Mobile Top 10 Risks

Lint

Conclusion

Index

Pearson